Claims

WHAT IS CLAIMED IS:

1. A method comprising:

attaching a secure router advertisement to an address update associated with a mobile node; and

sending the address update including the attached secure router advertisement to a correspondent node.

2. The method of claim 1 wherein the address update includes a Mobile IPv6-compliant binding update.

3. The method of claim 1 wherein the address update is sent by a node acting as a representative of the mobile node.

4. The method of claim 1 further comprising:

sending a secure router solicitation to one or more access routers; and

receiving the secure router advertisement, responsive to the secure router solicitation.

5. The method of claim 1 further comprising:

sending a secure router solicitation to one or more access routers, the secure router solicitation including an identifier of the mobile node; and

receiving the secure router advertisement responsive to the router solicitation, the secure router advertisement including the identifier of the mobile node.

6. The method of claim 1 wherein the mobile node is associated with a home address and further comprising:

sending a secure router solicitation to one or more access routers, the secure router solicitation including the home address of the mobile node; and

receiving the secure router advertisement responsive to the router solicitation, the secure router advertisement including the home address of the mobile node.

7. The method of claim 1 further comprising:

sending a router solicitation to one or more access routers, the secure router solicitation including a public key associated with the mobile node; and

receiving the secure router advertisement responsive to the router solicitation, the secure router advertisement including the public key.

8. The method of claim 1 wherein the secure router advertisement includes a signature of an access router associated with an access network, wherein the mobile node may receive one or more messages at an address that belongs to the access network of the access router.

9. The method of claim 1 wherein the secure router advertisement includes a signature of an access router associated with an access network, wherein a representative of the mobile node may receive one or more messages at an address that belongs to the access network of the access router.

10. The method of claim 1 wherein the mobile node is associated with a cryptographically-generated address generated by a public key and the secure router advertisement includes the same public key.

11. The method of claim 1 wherein the secure router advertisement includes a nonce field populated with an identifier of the mobile node.

12. The method of claim 1 wherein the secure router advertisement includes a nonce field populated with a home address of the mobile node.

13. The method of claim 1 wherein the secure router advertisement includes a nonce field populated with a public key associated with the mobile node.

14. The method of claim 1 wherein the mobile node is associated with a current address within an access network and the address update specifies the current address of the mobile node.

15. A computer program product encoding a computer program for executing on a computer system a computer process, the computer process comprising:

attaching a secure router advertisement to an address update associated with a mobile node; and

sending the address update including the attached secure router advertisement to a correspondent node.

16. The computer program product of claim 15 wherein the address update includes a Mobile IPv6-compliant binding update.

17. The computer program product of claim 15 wherein the address update is sent by a node acting as a representative of the mobile node.

18. The computer program product of claim 15 wherein the computer process further comprises:

sending a secure router solicitation to one or more access routers; and

receiving the secure router advertisement, responsive to the secure router solicitation.

19. The computer program product of claim 15 wherein the computer process further comprises:

sending a secure router solicitation to one or more access routers, the secure router solicitation including an identifier of the mobile node; and

receiving the secure router advertisement responsive to the router solicitation, the secure router advertisement including the identifier of the mobile node.

20. The computer program product of claim 15 wherein the mobile node is associated with a home address and the compute process further comprises:

sending a secure router solicitation to one or more access routers, the secure router solicitation including the home address of the mobile node; and

receiving the secure router advertisement responsive to the router solicitation, the secure router advertisement including the home address of the mobile node.

21. The computer program product of claim 15 wherein the computer process further comprises:

sending a router solicitation to one or more access routers, the secure router solicitation including a public key associated with the mobile node; and

receiving the secure router advertisement responsive to the router solicitation, the secure router advertisement including the public key.

22. The computer program product of claim 15 wherein the secure router advertisement includes a signature of an access router associated with an access network, wherein the mobile node may receive one or more messages at an address that belongs to the access network of the access router.

23. The computer program product of claim 15 wherein the secure router advertisement includes a signature of an access router associated with an access network, wherein a representative of the mobile node may receive one or more messages at an address that belongs to the access network of the access router.

24. The computer program product of claim 15 wherein the mobile node is associated with a cryptographically-generated address generated by a public key and the secure router advertisement includes the same public key.

25. The computer program product of claim 15 wherein the secure router advertisement includes a nonce field populated with an identifier of the mobile node.

26. The computer program product of claim 15 wherein the secure router advertisement includes a nonce field populated with a home address of the mobile node.

27. The computer program product of claim 15 wherein the secure router advertisement includes a nonce field populated with a public key associated with the mobile node.

28. The computer program product of claim 15 wherein the mobile node is associated with a current address within an access network and the address update specifies the current address of the mobile node.

29. A system comprising:

a node that attaches a secure router advertisement to an address update associated with a mobile node and sends the address update including the attached secure router advertisement to a correspondent node.

30. The system of claim 29 wherein the address update includes a Mobile IPv6-compliant binding update.

31. The system of claim 29 wherein the node is a representative of the mobile node.

32. The system of claim 29 wherein the node is the mobile node.

33. The system of claim 29 wherein the node transmits a secure router solicitation to one or more access routers.

34. The system of claim 29 wherein the secure router advertisement is generated by an access router responsive to the receipt of a secure router solicitation.

35. The system of claim 29 wherein the mobile node is associated with an identifier and the mobile node transmits a secure router solicitation to one or more access routers, the secure router solicitation including the identifier of the mobile node.

36. The system of claim 29 wherein the mobile node is associated with an identifier and the mobile node receives a secure router advertisement from an access router, the secure router advertisement including the identifier of the mobile node.

37. The system of claim 29 wherein the mobile node is associated with a home address and the mobile node transmits a secure router solicitation to one or more access routers, the secure router solicitation including the home address of the mobile node.

38. The system of claim 29 wherein the mobile node is associated with a home address and the mobile node receives a secure router advertisement from an access router, the secure router advertisement including the home address of the mobile node.

39. The system of claim 29 wherein the mobile node transmits a secure router solicitation to one or more access routers, the secure router solicitation including a public key of the mobile node.

40. The system of claim 29 wherein the mobile node receives a secure router advertisement from an access router, the secure router advertisement including a public key of the mobile node.

41. The system of claim 29 wherein the secure router advertisement includes a signature of an access router associated with an access network, wherein a mobile node is in the access network of the access router.

42. The system of claim 29 wherein the mobile node is associated with a cryptographically-generated address generated by a public key and the secure router advertisement includes the same public key.

43. The system of claim 29 wherein the secure router advertisement includes a nonce field populated with an identifier of the mobile mode.

44. The system of claim 29 wherein the secure router advertisement includes a nonce field populated with a home address of the mobile node.

45. The system of claim 29 wherein the secure router advertisement includes a nonce field populated with a public key associated with the mobile node.

46. The system of claim 29 wherein the mobile node is associated with a current address within an access network and the address update specifies the current address of the mobile node.

47. A method comprising:

receiving an address update from a mobile node, the address update including a secure router advertisement, a purported identifier of the mobile node, and a purported current address;

verifying that the secure router advertisement is signed by an authorized access router;

verifying that the purported current address is associated with the authorized access router; and

verifying the association between the purported identifier and the purported current address using data from the secure router advertisement.

48. The method of claim 47 wherein the mobile node is a Mobile IPv6 mobile node.

49. The method of claim 47 wherein the address update is a Mobile IPv6 binding update.

50. The method of claim 47 wherein the purported identifier is a Mobile IPv6 home address.

51. The method of claim 47 wherein the current address is a Mobile IPv6 care-of address.

52. The method of claim 47 wherein the operation of verifying the association between the purported identifier and the purported current address comprises:

reading an identifier from the secure router advertisement; and verifying that the purported identifier matches the identifier read from the secure router advertisement.

53. The method of claim 47 wherein the operation of verifying the association between the purported identifier and the purported current address comprises:

reading a home address from the secure router advertisement; and

verifying that the purported identifier matches the home address.

54. The method of claim 47 wherein the purported identifier is a cryptographically-generated address associated with the mobile node and the operation of verifying the association between the purported identifier and the current address comprises:

reading a public key from the secure router advertisement; and

verifying that the same public key was used to generate cryptographically-generated address.

55. The method of claim 47 wherein the authorized access router is associated with a subnet prefix specified in the secure router advertisement and the operation of verifying that the purported current address is associated with the authorized access router comprises:

verifying that the purported current address matches subnet prefix.

56. The method of claim 47 wherein the operation of verifying that the secure router advertisement is signed by an authorized access router comprises:

verifying that a signature used to sign the secure router advertisement is associated with an access router authorized by certification to advertise a subnet prefix specified in the secure router advertisement.

57. A computer program product encoding a computer program for executing on a computer system a computer process, the computer process comprising:

receiving an address update from a mobile node, the address update including a secure router advertisement, a purported identifier of the mobile node, and a purported current address;

verifying that the secure router advertisement is signed by an authorized access router;

verifying that the purported current address is associated with the authorized access router; and

verifying the association between the purported identifier and the purported current address using data from the secure router advertisement.

58. The computer program product of claim 57 wherein the mobile node is a Mobile IPv6 mobile node.

59. The computer program product of claim 57 wherein the address update is a Mobile IPv6 binding update.

60. The computer program product of claim 57 wherein the purported identifier is a Mobile IPv6 home address.

61. The computer program product of claim 57 wherein the current address is a Mobile IPv6 care-of address.

62. The computer program product of claim 57 wherein the operation of verifying the association between the purported identifier and the purported current address comprises:

reading an identifier from the secure router advertisement; and

verifying that the purported identifier matches the identifier read from the secure router advertisement.

63. The computer program product of claim 57 wherein the operation of verifying the association between the purported identifier and the purported current address comprises:

reading a home address from the secure router advertisement; and

verifying that the purported identifier matches the home address.

64. The computer program product of claim 57 wherein the purported identifier is a cryptographically-generated address associated with the mobile node

and the operation of verifying the association between the purported identifier and the current address comprises:

reading a public key from the secure router advertisement; and

verifying that the same public key was used to generate the cryptographically-generated address.

65. The computer program product of claim 57 wherein the authorized access router is associated with a subnet prefix specified in the secure router advertisement and the operation of verifying that the purported current address is associated with the authorized access router comprises:

verifying that the purported current address matches the subnet prefix.

66. The computer program product of claim 57 wherein the operation of verifying that the secure router advertisement is signed by an authorized access router comprises:

verifying that a signature used to sign the secure router advertisement is associated with an access router authorized by certification to advertise a subnet prefix specified in the secure router advertisement.

67. A system comprising:

a correspondent node that receives an address update from a mobile node, the address update including a secure router advertisement, a purported identifier of the mobile node, and a purported current address, the correspondent node verifying that the secure router advertisement is signed by an authorized access router, that the purported current address is associated with the authorized access router, and that data from the secure router advertisement associates the purported identifier with the purported current address.

68. The system of claim 67 wherein the mobile node is a Mobile IPv6 mobile node.

69. The system of claim 67 wherein the address update is a Mobile IPv6 binding update.

70. The system of claim 67 wherein the purported identifier is a Mobile IPv6 home address.

71. The system of claim 67 wherein the current address is a Mobile IPv6 care-of address.

72. The system of claim 67 wherein the correspondent nodes matches the purported identifier to an identifier read from the secure router advertisement.

73. The system of claim 67 wherein the correspondent nodes matches the purported identifier to a home address read from the secure router advertisement.

74. The system of claim 67 wherein the purported identifier is a cryptographically-generated address, the secure router advertisement includes a public key, and the correspondent verifies that the same public key was used to generate the cryptographically-generated address.

75. The system of claim 67 wherein the authorized access router is associated with a subnet prefix specified in the secure router advertisement and the correspondent node verifies that the purported current address matches the subnet prefix.

76. The system of claim 67 wherein the correspondent node verifies that a signature used to sign the secure router advertisement is associated with an access router authorized by certification to advertise a subnet prefix specified in the secure router advertisement.

77. One or more computer-readable media storing a data structure comprising:

a first data field storing a home address of a soliciting mobile node; and

a second data field storing a subnet prefix specifying an access network in which the mobile node is located.

78. The computer-readable media of claim 77 wherein the data structure further comprises:

a signature of an access router authorized to advertise the subnet prefix of the access network.

79. One or more computer-readable media storing a data structure comprising:

a first data field storing a public key of a soliciting mobile node; and

a second data field storing a subnet prefix specifying an access network in which the mobile node is located.

80. The computer-readable media of claim 79 wherein the data structure further comprises:

a signature of an access router authorized to advertise the subnet prefix of the access network.

81. One or more computer-readable media storing a data structure comprising:

a first data field storing a purported identifier of a mobile node;

a second data field storing a current address at which the mobile node is purported located; and

a third data field storing a secure router advertisement signed by an access router authorized to advertise the subnet prefix of the access network that includes the purported current address.

82. The computer-readable media of claim 81 wherein the purported identifier is a Mobile IPv6 home address.

83. The computer-readable media of claim 81 wherein the purported current address is a Mobile IPv6 care-of address.

84. The computer-readable media of claim 81 wherein the purported identifier is a public key.

85. The computer-readable media of claim 81 wherein the secure router advertisement includes the purported identifier in the nonce field.

86. A computer program product encoding a computer program for executing on a computer system a computer process, the computer process comprising:

generating a secure router advertisement data structure, wherein a nonce field of the a secure router advertisement data structure contains a member of a set containing an IPv6 address, a home address, an identifier, a group identifier, a cryptographic identifier, and a public key.